The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
11/3/2010
11/4/2010 - ***Updated***

SUBJECT:
Vulnerability in Internet Explorer Could Allow Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of the vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability and there are reports that it is being exploited for targeted attacks.

UPDATED OVERVIEW:
Proof-of-concept code has been made publically available for this vulnerability.

A patch is still not available, however Microsoft has released a Fix it solution that automates the work around process of enabling DEP for IE 7 and is discussed in the 'Frequently Asked Question' section of the Microsoft advisory. Please see the Microsoft advisory in references for additional information.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

ORIGINAL DESCRIPTION:

A new vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. This issue arises when a certain combination of Cascading Style Sheet (CSS) tags are stored which may result in a use-after-free condition. A use-after-free condition occurs when an application deallocates a memory block and then later attempts to access that deallocated space.

Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of the vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability and there are reports that it is being exploited for targeted attacks.

UPDATED DESCRIPTION:
Proof-of-concept code has been made publically available for this vulnerability.

A patch is still not available, however Microsoft has released a Fix it solution that automates the work around process of enabling DEP for IE 7 and is discussed in the 'Frequently Asked Question' section of the Microsoft advisory. Please see the Microsoft advisory in references for additional information.

RECOMMENDATIONS:

The following actions should be taken:

Consider implementing the following workarounds as listed by Microsoft:

- Override the Web site CSS style with a user defined CSS.
- Deploy the Enhanced Mitigation Experience Toolkit.
- Enable Data Execution Prevention for IE 7.
- Read email in plain-text format.
- Set Internet and Local Intranet security zone settings to high to block ActiveX controls and Active Scripting.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- If you have an alternate browser deployed, consider using it until this vulnerability is remediated.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/advisory/2458511.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3962

Symantec:
http://www.symantec.com/connect/blogs/new-ie-0-day-used-targeted-attacks

SANS:
http://isc.incidents.org/diary.html?storyid=9874

Security Focus:
http://www.securityfocus.com/bid/44536